Fact Sheet

Preventing Provider Medical Identity Theft

Physicians, other providers, and beneficiaries of Medicare and Medicaid are at risk for medical identity theft. The Centers for Medicare & Medicaid Services (CMS) is working to raise awareness among providers and help them protect their medical identities. "Medical identity theft is the appropriation or misuse of a patient's or [provider's] unique medical identifying information to obtain or bill public or private payers for fraudulent medical goods or services."[1]

Common Provider Medical Identity Theft Schemes

A common provider medical identity theft scheme involves a fraudster billing services directly in a physician's or other provider's name even though these individuals never provided the service. Another common scheme is using physician and other provider medical identifiers to refer patients for additional services and supplies, such as home health services, diagnostic testing, and medical equipment and supplies that were not ordered by the physician or not delivered or provided to the beneficiary.[2]

Main Provider Risk Factors

The primary risk factor for medical identity theft is provider complicity (providers' intentional, voluntary misuse or abuse of their medical identifiers) in fraud schemes. Providers who voluntarily permit misuse of their identifiers place this information at significant risk for subsequent theft and can create unintended consequences. Common examples of ways providers allow the misuse of medical identifiers include signing referrals for patients they do not know, signing Certificates of Medical Necessity (CMNs) for patients who do not need the service or supply, signing CMNs for more services than what patients actually need, and even signing blank referral forms. Purposeful misuse of medical identifiers can lead to significant consequences, such as civil monetary penalties, criminal fines and restitution, prison time, and

exclusion from Medicare and Medicaid. Physicians (and other providers) can be held liable for these actions even without evidence of other fraud.[3]

In addition to provider complicity and the voluntary misuses of medical identifiers, honest providers can fall victim to identity theft because of inherent structural risks in the health care industry associated with provider medical identifiers. Public access to National Provider Identifiers and provider license numbers is one such risk. Other risks include the expectation by an organization for providers to disclose identifiers when they apply for positions. The more parties with access to a provider's medical identifiers, the greater the risk of exposure for medical identity theft by unscrupulous individuals. Examples of high-risk exposure include reassigning medical identifiers for billing purposes, providing medical identifiers to staff, and allowing mid-level practitioners to use the supervising provider's medical identifiers.

Penalties for Identity Theft

In December 2015, the Patient Access and Medicare Protection Act became law. Section 8 of the law amended section 1128B(b) of the Social Security Act to stiffen penalties for provider and beneficiary identity theft. If anyone without proper authority "knowingly and willfully purchases, sells or distributes, or arranges for the purchase, sale, or distribution" of any beneficiary or provider identification number under Medicare, Medicaid, or Children's Health Insurance Programs, the maximum penalties are 10 years in prison, a $500,000 fine for individuals or $1,000,000 for corporations, or both. Of course, other criminal and civil statutes will apply if the misappropriated identifiers are used to submit fraudulent claims.[4]

Mitigate Risk

Providers are responsible for their medical identifiers to the extent they can protect them and mitigate their vulnerability to theft. Four strategies providers can use to protect themselves and their practices include:

- Actively managing enrollment information with payers by updating enrollment changes, especially when opening, closing, or moving practice locations; when separating from an organization; or when changing banking information;
- Monitoring billing and compliance processes by strengthening policies and procedures to minimize risks and improve overall program integrity. Policies and procedures might include adopting sound billing practices (for example, reviewing remittance notices), carefully reading documents before signing them, and limiting and monitoring third party use of medical identifiers;

- Controlling unique medical identifiers by taking steps, such as thoroughly training staff on all policies and procedures, screening employees, securing all information technology, and keeping track of all prescription pads; and
- Engaging patients in conversation about the risks of medical identity theft by explaining the impact it can have on them and their medical records, educating them on the signs of potential identity theft, and warning them of the dangers of card sharing.[5]

Remediation for Victims

The Center for Program Integrity's (CPI's) goal is to proactively identify and help identity theft victims. CPI can:

- Help absolve related debts, such as overpayments and tax obligations; and
- Respond to the needs of legitimate providers.

For additional CPI information, visit https://www.cms.gov/Medicare-Medicaid-Coordination/Fraud-Prevention/MedicaidIntegrityProgram/Downloads/cpiinitiatives.pdf on the CMS website.

Report It

To report fraud and abuse:

- Contact local law enforcement (visit http://www.naag.org on the National Association of Attorneys General website for local law enforcement and consumer protection information). Also notify credit reporting companies.
- Contact your State Medicaid Fraud Control Unit or State Medicaid agency. Their contact information can be found at https://www.cms.gov/medicare-medicaid-coordination/fraud-prevention/fraudabuseforconsumers/report_fraud_and_suspected_fraud.html on the CMS website.
- Contact the Federal Trade Commission:

  Federal Trade Commission
  600 Pennsylvania Avenue, NW
  Washington, DC 20580
  Phone: 1-877-438-4338 (1-877-ID THEFT)
  TTY: 1-866-653-4261
  Website: https://www.consumer.ftc.gov/features/feature-0014-identity-theft

- Contact the U.S. Department of Health and Human Services, Office of Inspector General:

  Office of Inspector General
  U.S. Department of Health and Human Services
  ATTN: Hotline
  P.O. Box 23489
  Washington, DC 20026
  Phone: 1-800-HHS-TIPS (1-800-447-8477)
  TTY: 1-800-377-4950
  Fax: 1-800-223-8164
  Email: HHSTips@oig.hhs.gov
  Website: https://forms.oig.hhs.gov/hotlineoperations/

Resources

To see the electronic version of this fact sheet and the other products included in the "Safeguarding Your Medical Identity" Toolkit, visit the Medicaid Program Integrity Education page at https://www.cms.gov/Medicare-Medicaid-Coordination/Fraud-Prevention/Medicaid-Integrity-Education/edmic-landing.html on the CMS website.

Follow us on Twitter #MedicaidIntegrity

References

1 Agrawal, S., & Budetti, P. (2012, February 1). Physician Medical Identity Theft. The Journal of the American Medical Association, 307(5), 459–460. Retrieved February 29, 2016, from http://jama.jamanetwork.com/article.aspx?articleid=1104942

2 Agrawal, S., & Budetti, P. (2012, February 1). Physician Medical Identity Theft. The Journal of the American Medical Association, 307(5), 459–460. Retrieved February 29, 2016, from http://jama.jamanetwork.com/article.aspx?articleid=1104942

3 Agrawal, S., & Budetti, P. (2012, February 1). Physician Medical Identity Theft. The Journal of the American Medical Association, 307(5), 459–460. Retrieved February 29, 2016, from http://jama.jamanetwork.com/article.aspx?articleid=1104942

4 U.S. Congress. (2015, December 28). Patient Access and Medicare Protection Act. Retrieved March 9, 2016, from https://www.congress.gov/bill/114th-congress/senate-bill/2425/text?q=%7B%22search%22%3A%5B%22medicare+identity+theft%22%5D%7D&resultIndex=2

5 Medicare Learning Network. (2014, October). Medicaid Program Integrity: Understanding Provider Medical Identity Theft. Retrieved February 29, 2016, from https://www.cms.gov/Outreach-and-Education/Medicare-Learning-Network-MLN/MLNProducts/Downloads/Med-ID-Theft-Booklet-ICN908264.pdf

Disclaimer

This fact sheet was current at the time it was published or uploaded onto the web. Medicaid and Medicare policies change frequently so links to the source documents have been provided within the document for your reference.

This fact sheet was prepared as a service to the public and is not intended to grant rights or impose obligations. This fact sheet may contain references or links to statutes, regulations, or other policy materials. The information provided is only intended to be a general summary. Use of this material is voluntary. Inclusion of a link does not constitute CMS endorsement of the material. We encourage readers to review the specific statutes, regulations, and other interpretive materials for a full and accurate statement of their contents.

April 2016